特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004年11月4日 (04.11.2004)

PCT

(10) 国際公開番号
WO 2004/095772 A1

(51) 国際特許分類[7]: H04L 9/32, G06F 15/00

(21) 国際出願番号: PCT/JP2004/005741

(22) 国際出願日: 2004年4月21日 (21.04.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-115755 2003年4月21日 (21.04.2003) JP
特願2003-188141 2003年6月30日 (30.06.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 三浦 貴之 (MIURA, Takayuki) [JP/JP]. 小野 剛 (ONO, Tsuyoshi) [JP/JP]. 鈴木 直志 (SUZUKI, Naoshi) [JP/JP]. 宮田 耕自 (MIYATA, Kouji) [JP/JP].

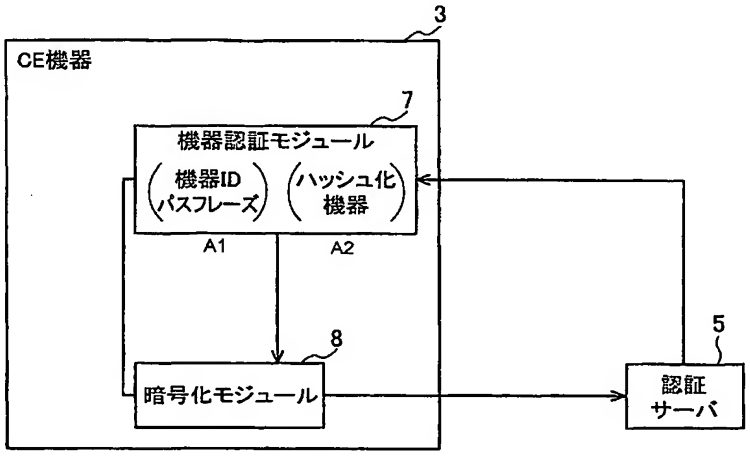
(74) 代理人: 中村 友之 (NAKAMURA, Tomoyuki); 〒1050001 東京都港区虎ノ門１丁目２番３号虎ノ門第一ビル９階 三好内外国特許事務所内 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,

[続葉有]

(54) Title: DEVICE AUTHENTICATION SYSTEM

(54) 発明の名称: 機器認証システム



3...CE DEVICE
7...DEVICE AUTHENTICATION MODULE
A1...DEVICE ID, PATH PHRASE
A2...HASHING DEVICE
8...ENCRYPTION MODULE
5...AUTHENTICATION SERVER

(57) Abstract: In a CE device, it is possible to connect a device authentication module with an encryption module by a dynamic link. An authentication server (5) generates a random number. A device authentication module (7) creates a digest by combining a path phrase with this random number and transmits the digest and the device ID to an encryption module (8). The encryption module encrypts the communication path and transmits these information to an authentication server (5). The authentication server (5) searches the path phrase from the device ID and combines this with the random number previously generated, thereby creating a digest. This digest is compared to the digest received from the encryption module (8), thereby performing device authentication. The encryption module (8) can be connected by a dynamic link instead of a static link so as to receive a digest instead of a path phrase from the device authentication module (7).

(57) 要約: ＣＥ機器において、機器認証モジュールと暗号化モジュールをダイナミックリンクにて接続できるようにすること。認証サーバ（５）で乱数を発生させる。機器認証モジュール（７）はパスフレーズとこの乱数を組み合わせてダイジェ

[続葉有]

WO 2004/095772 A1

LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

ストを生成し、これと機器ＩＤを暗号化モジュール（８）に渡す。暗号化モジュールは、通信経路を暗号化し、これらの情報を認証サーバ（５）に送信する。認証サーバ（５）は、機器ＩＤからパスフレーズを検索し、これと先に生成した乱数を組み合わせてダイジェストを生成する。このダイジェストと暗号化モジュール（８）から受信したダイジェストを比較して機器認証を行う。暗号化モジュール（８）は、機器認証モジュール（７）からパスフレーズではなくダイジェストを受け取るため、スタティックリンクにて接続せずにダイナミックリンクで接続することができる。

明　細　書

機器認証システム

機器認証システム、端末機器、認証サーバ、サービスサーバ、端末機器方法、認証方法、端末機器プログラム、認証プログラム、サービスサーバプログラム、及び記憶媒体

技術分野

本発明は、認証システムなどに関し、特に、セキュリティ上重要な情報を所定のロジックで変換し、変換後の情報を用いて認証するものに関する。

背景技術

近年、ＣＥ（ＣＥ：Ｃｏｎｓｕｍｅｒ　Ｅｌｅｃｔｒｏｎｉｃｓ）機器の普及が広まりつつある。ＣＥ機器とは、例えば、ビデオデッキ、ハードディスクレコーダ、ステレオ、テレビなどのオーディオビジュアル機器や、パーソナルコンピュータ、デジカメ、カムコーダ、ＰＤＡ、ゲーム機、ホームルータ等の電子機器や、炊飯器、冷蔵庫などの家電製品や、その他の電子機器にコンピュータを内蔵させ、ネットワークを介したサービスを利用できるものである。

そして、ＣＥ機器からサーバにアクセスしてコンテンツをダウンロードしたり、サービスを受けるなどし、ユーザはサーバが提供するサービスを利用することができる。

サーバが提供するサービスには、ＣＥ機器全般に提供するものと、機器認証された特定のＣＥ機器に提供するものがある。

サーバは、機器認証を要するサービスを提供する場合、そのＣＥ機器

を認証サーバで認証し、認証された場合にサービスを提供する。

このように、サービスサーバが端末機器にサービスを提供するものとして次の発明がある。

特許文献１：特開２００２－３４２２８５号公報

この発明は、端末機器（携帯電話）から認証要求があった場合に、これを認証すると共に端末機器にワンタイムパスワードを発行して送信する。端末機器から情報の要求があった場合、端末機器から先のワンタイムパスワードを受信し、認証したのが確かにこの端末機器であるかを確認するものである。

図１２は、従来のＣＥ機器１０１の構成を示した図である。ＣＥ機器１０１は、機器ＩＤやパスフレーズなどの認証に必要な認証情報を記憶していると共に、機器認証に関する処理を行う機器認証モジュール１０３と、機器認証モジュール１０３から認証情報を受け取り、通信経路を暗号化してこれを機器認証先１０５に送信する暗号化モジュール１０４を備えている。

機器認証モジュール１０３は、暗号化モジュール１０４に認証情報を平文で渡すため、この認証情報が第三者に読み取られないように、機器認証モジュール１０３と暗号化モジュール１０４はスタティックリンクにて結合されている。

通信経路を暗号化するモジュールは、機器認証以外の用途で利用する場合も多いが、暗号化モジュール１０４は機器認証モジュール１０３とスタティックリンクされているため、ＣＥ機器１０１は、これとは別に機器認証以外の用途で使用する暗号化モジュールを用意している。

このように、ＣＥ機器１０１では、同じ機能を有する２つの暗号化モジュールをＣＥ機器１０１内のメモリに実装しなくてはならず、実質として機器認証モジュールの容量が多くなり、ＣＥ機器１０１の利用可能な

メモリ領域を圧迫したり、あるいは機器認証機能の実装そのものが困難となる場合があった。

そこで、本発明の目的は、端末機器内のメモリを有効利用することができる機器認証機能を実現できる端末機器認証システムなどを提供することである。

発明の開示

機器認証用の秘密情報を備えた端末機器と、前記秘密情報とを用いて前記端末機器の機器認証を行う認証サーバから構成された機器認証システムであって、前記端末機器は、乱数を取得し、前記取得した乱数と前記秘密情報との組を一方向性関数により変換して変換値を生成し、前記認証サーバは、前記端末機器が取得した乱数、前記端末機器の秘密情報、及び前記端末機器が生成した変換値を取得し、前記取得した乱数と秘密情報との組を前記端末機器が用いた一方向性関数と同じ一方向性関数により変換して変換値を生成し、前記端末機器装置において生成した変換値と、前記認証サーバにおいて生成した変換値を比較することにより前記端末機器の機器認証を行うことを特徴とする機器認証システムを提供する（第１の構成）。

また、本発明は、第１の構成の機器認証システムで機器認証を受ける端末機器が、認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、を具備するように構成することもできる（第２の構成）。

また、本発明は、第２の構成の端末機器を機器認証する認証サーバが、

乱数を取得する乱数取得手段と、前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に送信する送信手段と、前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受信する受信手段と、前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定手段と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換手段と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、を具備するように構成することもできる（第３の構成）。

また、本発明は、第１の構成の機器認証システムが、認証サーバによる認証を経て前記端末機器にサービスを提供するサービスサーバを含み、前記サービスサーバが、乱数を取得する乱数取得手段と、前記取得した乱数を端末機器に送信する乱数送信手段と、前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信手段と、前記端末機器に送信した乱数を特定する乱数特定手段と、前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信手段と、前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信手段と、を具備するように構成することもできる（第４の構成）。

また、本発明は、第４の構成のサービスサーバからサービスの提供を受ける端末機器が、サービスサーバから乱数を受信する乱数受信手段と、前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、を具備するように構成することもできる（第５の構成）。

また、本発明は、第４の構成のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバが、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信手段と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、前記受信した乱数と前記特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換手段と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、を具備するように構成することもできる（第６の構成）。

また、本発明は、第１の構成の機器認証システムで機器認証を受ける端末機器で用いる端末機器方法であって、前記端末機器は、受信手段と、変換手段と、送信手段と、備えたコンピュータから構成されており、認証サーバから、乱数と当該乱数を特定する乱数特定情報を前記受信手段で受信する受信ステップと、前記受信した乱数と秘密情報の組を一方向性関数により前記変換手段で変換して変換値を生成する変換ステップと、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、から構成された端末機器方法を提供する。

また、本発明は、第２の構成の端末機器を機器認証する認証サーバで用いる認証方法であって、前記認証サーバは、乱数取得手段と、送信手段と、受信手段と、乱数特定手段と、秘密情報特定手段と、変換手段と、機器認証手段と、を備えたコンピュータから構成されており、前記乱数取得手段で乱数を取得する乱数取得ステップと、前記取得した乱数と、当該乱数を特定する乱数特定情報を前記送信手段で端末機器に送信する送信ステップと、前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を前記受信手段で受信する受信ステップと、前記受信

した乱数特定情報を用いて前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を前記秘密情報特定手段で特定する秘密情報特定ステップと、前記特定した秘密情報と乱数の組を、前記変換手段で前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、前記受信した変換値と前記生成した変換値を用いて前記機器認証手段で前記端末機器を機器認証する機器認証ステップと、から構成された認証方法を提供する。

また、本発明は、第４の構成のサービスサーバで用いる認証方法であって、前記サービスサーバは、乱数取得手段と、乱数送信手段と、受信手段と、乱数特定手段と、認証情報送信手段と、認証結果受信手段と、を備えたコンピュータから構成されており、前記乱数取得手段で乱数を取得する乱数取得ステップと、前記取得した乱数を前記乱数送信手段で端末機器に送信する乱数送信ステップと、前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を前記受信手段で受信する受信ステップと、前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を前記認証情報送信手段で認証サーバに送信する認証情報送信ステップと、前記認証サーバから前記送信した認証情報による認証結果を前記認証結果受信手段で受信する認証結果受信ステップと、から構成された認証方法を提供する。

また、本発明は、第４の構成のサービスサーバからサービスの提供を受ける端末機器で用いる端末機器方法であって、前記端末機器は、乱数受信手段と、変換手段と、送信手段とを備えたコンピュータから構成されており、前記乱数受信手段でサービスサーバから乱数を受信する乱数受信ステップと、前記受信した乱数と、秘密情報の組を前記変換手段で

一方向性関数により変換して変換値を生成する変換ステップと、前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、から構成された端末機器方法を提供する。

また、本発明は、第４の構成のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバが用いる認証方法であって、前記認証サーバは、受信手段と、秘密情報特定手段と、変換手段と、機器認証手段と、を備えたコンピュータから構成されており、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を前記受信手段で受信する受信ステップと、前記秘密情報特定手段で、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定ステップと、前記受信した乱数と前記特定した秘密情報との組を前記変換手段で前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、前記機器認証手段で、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証ステップと、から構成された認証方法を提供する。

また、本発明は、第１の構成の機器認証システムで機器認証を受けるコンピュータで構成された端末機器において、認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信機能と、前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換機能と、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、を実現する端末機器プログラムを提供する。

また、本発明は、第２の構成の端末機器を機器認証するコンピュータで構成された認証サーバにおいて、乱数を取得する乱数取得機能と、前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に送信

する送信機能と、前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受信する受信機能と、前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定機能と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換機能と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、を実現する認証プログラムを提供する。

また、本発明は、第４の構成のコンピュータで構成されたサービスサーバにおいて、乱数を取得する乱数取得機能と、前記取得した乱数を端末機器に送信する乱数送信機能と、前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信機能と、前記端末機器に送信した乱数を特定する乱数特定機能と、前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信機能と、前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信機能と、を実現するサービスサーバプログラムを提供する。

また、本発明は、第４の構成のサービスサーバからサービスの提供を受けるコンピュータで構成された端末機器において、サービスサーバから乱数を受信する乱数受信機能と、前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換機能と、前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、を実現する端末機器プログラムを提供する。

また、本発明は、第４の構成のサービスサーバがサービスを提供する

際に、端末機器を機器認証するコンピュータで構成された認証サーバにおいて、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信機能と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、前記受信した乱数と前記特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換機能と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、を実現する認証プログラムを提供する。

また、本発明は、上記各プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。

また、本発明は、請求項１の機器認証システムで機器認証を受ける端末機器であって、認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、を具備し、前記秘密情報と、前記変換手段は、端末機器に組み込まれた耐タンパ装置に格納されていることを特徴とする端末機器を提供する。

図面の簡単な説明

図１は、本実施の形態の機器認証システムの構成を説明するための図である。

図２は、ＣＥ機器の機器認証に関する構成要素を説明するための図である。

図３は、ＣＥ機器のハードウェア的な構成の一例を示した図である。

図４は、機器認証を行う手順を説明するためのフローチャートであ

る。

図５は、ダイジェスト認証処理の手順を説明するためのフローチャートである。

図６は、サービスサーバが認証サーバで認証結果を確認する手順を説明するためのフローチャートである。

図７は、ＣＥ機器が認証サーバを確認する別のシーケンスを説明するためのフローチャートである。

図８は、機器認証を行う他の手順を説明するためのフローチャートである。

図９は、ダイジェスト認証処理の手順を説明するためのフローチャートである。

図１０は、本実施の形態の変形例を説明するための図である。

図１１は、本変形例のハードウェア的な構成の一例を示した図である。

図１２は、従来のＣＥ機器の構成を説明するための図である。

発明を実施するための最良の形態

以下、本発明の好適な実施の形態について、図を参照して詳細に説明する。

（１）実施形態の概要

図２に示したように、機器認証モジュール７は、認証サーバ５からサーバ乱数とワンタイムＩＤを受信し、このサーバ乱数とパスフレーズを組み合わせてハッシュ化してダイジェストを生成する。そして、これを機器ＩＤと共に暗号化モジュール８に渡す。暗号化モジュール８は、通信経路を暗号化し、ダイジェストと機器ＩＤ、及びワンタイムＩＤを認

証サーバ５に送信する。

認証サーバ５は、予め機器ＩＤとＣＥ機器３のパスフレーズを対応付けて記憶している。また、先にＣＥ機器３に送信したサーバ乱数とワンタイムＩＤを対応付けて記憶している。

認証サーバ５は、ＣＥ機器３から受信したワンタイムＩＤと機器ＩＤを用いてパスフレーズと先に発生したサーバ乱数を特定する。そしてこれらを組み合わせ、ＣＥ機器３側のロジックと同じロジックでダイジェストを生成する。そして、生成したダイジェストとＣＥ機器３から受信したダイジェストを照合し、両者が一致するか否かでＣＥ機器３の認証を行う。

このように、機器認証モジュール７は、暗号化モジュール８にパスフレーズを渡さずに、サーバ乱数とパスフレーズの組から生成したダイジェストを渡す。そのため、機器認証モジュール７から第三者によりダイジェストが読み取られたとしても第三者はダイジェストからパスフレーズを復元することはできない。

更に、認証サーバ５は、機器認証の度に異なるサーバ乱数を生成するため、機器認証モジュール７が暗号化モジュール８に渡すダイジェストも機器認証ごとに異なり、例えダイジェストが第三者に読み取られたとしてもこれを乱用されることはない。

また、機器認証の度に同じダイジェストを用いる第三者にこのダイジェストが漏れた場合、これを元に所謂リプレイ攻撃が行われる可能性があるが、ＣＥ機器３は、機器認証の度に異なるダイジェストを生成するのでリプレイ攻撃されることはない。

（２）実施形態の詳細

図１は、本実施の形態の機器認証システム１の構成を説明するための図である。

機器認証システム１は、ＣＥ機器３、サービスサーバ４、認証サーバ５がネットワークを介して通信可能に接続されている。

なお、図１ではＣＥ機器３とサービスサーバ４が一台ずつ記載されているが、これは複数存在させることができる。

ＣＥ機器３は、機器ＩＤ、パスフレーズなど機器認証に必要な認証情報を備えており（記憶装置３ａに記憶してある、図３の記憶部２８に対応）、これらの情報を用いて認証サーバ５で機器認証を受け、サービスサーバ４が提供するサービスを利用することができる。

なお、パスフレーズは、ＣＥ機器３と認証サーバ５が機器認証のために共有する秘密情報を構成している。

サービスサーバ４は、ＣＥ機器３に、例えば、コンテンツを送信するなどサービスを提供するサーバである。サービスサーバ４が提供するサービスには機器認証を要するものと要しないものがある。ＣＥ機器３が機器認証を要するサービスを要求した場合、サービスサーバ４は、認証サーバ５に機器認証を代行してもらう。

サービスサーバ４は、サービスを提供するＣＥ機器３を登録してあり、サービスサーバ４に接続可能な各ＣＥ機器の機器情報（シリアルナンバなど）、保有者情報などを記憶装置４ａに記憶している。これらの情報は、ＣＥ機器３から認証結果を受信した際に、認証サーバ５に機器認証を受けたＣＥ機器３が本当にこのＣＥ機器３であるか確認するのに用いる。

認証サーバ５は、サービスサーバ４に代わってＣＥ機器３の機器認証を代行するサーバである。

認証サーバ５は、乱数（以下、サーバ乱数と呼ぶことにする）を生成してＣＥ機器３に送信し、ＣＥ機器３から機器ＩＤ、及びサーバ乱数とパスフレーズから生成したダイジェストなどを受信し、ＣＥ機器３の機

器認証を行う。認証サーバ５は、認証ごとに毎回異なったサーバ乱数を生成する。

認証サーバ５は、乱数を発生させることによりこれを取得する乱数取得手段を備えているが、認証サーバ５は、他の装置が生成した乱数取得するように構成することもできる。

認証サーバ５は、各ＣＥ機器３ごとにパスフレーズ、機器ＩＤ、機器情報、保有者情報などを記憶装置５ａに記憶しているほか、サービスサーバ４がＣＥ機器３にサービスを提供するサービスサイトのＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒｓ）も記憶している。このＵＲＬは、ＣＥ機器３が利用しようとしているサイトが適切なものか否かを判断するために、予めサービスサーバ４が取得して登録したものである。

認証サーバ５は、ＣＥ機器３から機器ＩＤを受信、この機器ＩＤにひも付けられたパスフレーズを検索することにより、ＣＥ機器３のパスフレーズを取得する。このように、機器ＩＤはＣＥ機器３の秘密情報（パスフレーズ）を特定する秘密情報特定情報を構成している。

サービスサーバ４のほかに機器認証を行う認証サーバ５を設けたのは（従来はサービスサーバ４が機器認証も行っていた）、サービスサーバ４は一般の個人や任意の団体などが運営する場合も多く、認証情報をサービスサーバ４に提供した場合、提供した情報が悪用されてしまう可能性があるためである。

このように、機器認証の代行を行う認証サーバ５を設けたシステムとしては未公開の文献（特願２００２－１４４８９６）で提案されているサービス提供システムがある。

このシステムでは、機器認証を機器認証サーバが一括して行い、サービスサーバは、機器認証サーバでの認証結果を受け取って、ＣＥ機器に

サービスを提供するか否かを判断する。

このシステムでは、機器認証を行う場合にセキュリティ上重要な情報を機器認証サーバに送信するため、これらの情報をサービスサーバに提供する必要がない。

図２は、ＣＥ機器３を構成する要素のうち、機器認証に関するものを説明するための図である。

ＣＥ機器３は、機器認証モジュール７と暗号化モジュール８を備えている。機器認証モジュール７は、機器ＩＤやパスフレーズなど、機器認証に必要な認証情報を記憶している。また、機器認証モジュール７は、認証サーバ５からサーバ乱数の受信し、これとパスフレーズを組み合わせてハッシュ化し、ダイジェスト（ハッシュ値、あるいはダイジェストメッセージ）を生成することができる。

機器認証モジュール７は、認証情報として機器ＩＤとダイジェストを暗号化モジュール８に渡す。

ここでハッシュ化とは、ハッシュ関数と呼ばれる関数を用いて電子文書から文字列（ダイジェスト）を生成する処理のことである。

同じ電子文書からは同じダイジェストが得られる。電子文書が一部でも変更されると、この文書のダイジェストは、変更前のものと異なる。また、ダイジェストから元の電子文書を復元することはできない。

なお、ハッシュ関数は一方向性関数と呼ばれる関数の一種である。一方向性関数とは、変換元から変換値への変換は容易であるが、変換値から変換元への逆変換が困難な関数である。そして、ダイジェストは、変換元（パスフレーズとサーバ乱数の組）をハッシュ関数で変換した変換値となる。

このように、ＣＥ機器３は、乱数（サーバ乱数）と秘密情報（パスフレーズ）の組を一方向性関数で変換し変換値（ダイジェスト）を取得す

る変換手段を備えている。

暗号化モジュール８は、例えば、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ）などの暗号化技術を使って、通信経路を暗号化するモジュールである。暗号化モジュール８は、機器認証モジュール７から認証情報を受け取り、暗号化した通信経路を経由して認証サーバ５に認証情報を送信する。

このように、ＣＥ機器３では、機器認証モジュール７から出力されるパスフレーズは、サーバ乱数と組にして生成されたダイジェストとなっている。そのため、機器認証モジュール７から暗号化モジュール８に渡される認証情報には、平文のパスフレーズが含まれておらず、認証情報が第三者に渡ったとしても、ダイジェストからパスフレーズを復元することはできない。更に、機器認証に使用するダイジェストは毎回変化するので、第三者がダイジェストを読み取ってもこれを乱用することはできない。そのため高いセキュリティを確保することができる。

機器認証モジュール７と暗号化モジュール８は、ダイナミックリンクにより接続される。

即ち、暗号化モジュール８は、機器認証モジュール７が認証情報を認証サーバ５に送信する際に暗号化モジュール８に動的に接続される。

そのため、暗号化モジュール８は、機器認証モジュール７とは別の通信経路を暗号化する必要があるモジュールからも利用できる。

その場合は、そのモジュールが暗号化した通信経路で情報を送信する場合に暗号化モジュール８が動的にそのモジュールに接続する。

このように、暗号化モジュール８は、複数のモジュールから共用することができ、ＣＥ機器３のメモリ領域を節約することができる。

図３は、ＣＥ機器３のハードウェア的な構成の一例を示した図である。

ＣＰＵ(Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ)２１は、

ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２２に記憶されているプログラム、または記憶部２８からＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）２３にロードされたプログラムに従って各種の処理を実行する。

また、ＲＡＭ２３には、ＣＰＵ２１が各種の処理を実行する上で必要なデータなども適宜記憶されている。

ＣＰＵ２１、ＲＯＭ２２、およびＲＡＭ２３は、バス２４を介して相互に接続されている。このバス２４には、入出力インターフェース２５も接続されている。

入出力インターフェース２５には、キーボード、マウスなどよりなる入力部２６、ＣＲＴ（Ｃａｔｈｏｄｅ－ｒａｙ　Ｔｕｂｅ）、ＬＣＤ（Ｌｉｑｕｉｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）などよりなるディスプレイ、並びにスピーカなどによりなる出力部２７、ハードディスクなどにより構成される記憶部２８、モデム、ターミナルアダプタなどにより構成される通信部２９が接続されている。通信部２９は、ネットワークを介しての通信処理を行う。

また、入出力インターフェース２５には、必要に応じてドライブ３０が接続され、磁気ディスク４１、光ディスク４２、光磁気ディスク４３、またはメモリカード４４などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて記憶部２８にインストールされる。

なお、認証サーバ５、サービスサーバ４の構成は基本的にＣＥ機器３と同様であるので説明は省略する。

図４は、ＣＥ機器３が認証サーバ５から機器認証を受ける手順を説明するためのフローチャートである。

なお、ＣＥ機器３は、認証サーバ５の公開鍵を備えており、認証サー

バ５は対応する秘密鍵を備えているものとする。

また、ＣＥ機器３と認証サーバ５は、フローチャート中の括弧で示した各手段を備えている。

ＣＥ機器３がサービスサーバ４で機器認証が必要なサービスにアクセスすると、サービスサーバ４がＣＥ機器３に機器認証トリガを送信する（ステップ４０）。

この機器認証トリガは、ＣＥ機器３に機器認証動作を開始させるための情報であり、認証サーバ５のＵＲＬや、サービスサイトが要求する認証のバージョンなどの情報が含まれている。

なお、機器認証にはいくつかのバージョンが用意されており、バージョンにより利用できるサービスが異なる場合がある。

ＣＥ機器３は、サービスサーバ４から認証トリガを受信する。

以下の、ＣＥ機器３と認証サーバ５の通信は、暗号化モジュール８で暗号化された通信経路を介して行われる。

ＣＥ機器３は、認証トリガに含まれる認証サーバ５のＵＲＬを用いて認証サーバ５に接続し、サーバ乱数の送信を要求する（ステップ２）。

また、このとき、ＣＥ機器３は、認証トリガに含まれているサービスサーバ４が要求するバージョンと、ＣＥ機器３が実装している機器認証のバージョンを認証サーバ５に送信する。

認証サーバ５は、ＣＥ機器３からサーバ乱数の送信要求を受信し、サーバ乱数を発生させる（乱数取得手段）（ステップ２０）。また、サービスサーバ４が要求しているバージョンとＣＥ機器３のバージョンが一致しているか否かの確認も行う。

更に、認証サーバ５は、ワンタイムＩＤ１を生成する。そして、サーバ乱数とワンタイムＩＤ１をＣＥ機器３に送信する（送信手段）（ステップ２２）。

なお、サービスサーバ４は後ほど別のワンタイムＩＤを生成するが、これと区別するため、上記のワンタイムＩＤをワンタイムＩＤ１とし、後に生成するワンタイムＩＤをワンタイムＩＤ２とする。

このワンタイムＩＤ１は、ＣＥ機器３と認証サーバ５でセッションを維持するために使用される使い捨てのＩＤである。

認証サーバ５は、ＣＥ機器３からワンタイムＩＤ１を受信することによりＣＥ機器３と維持しているセッションを認識することができる。

ワンタイムＩＤ１は、機器認証ごとに異なる値が発行されるので、高いセキュリティを確保することができる。

また、認証サーバ５は、送信したサーバ乱数とワンタイムＩＤ１をひも付けして記憶する。これにより、後にＣＥ機器３からワンタイムＩＤ１を受信することにより、ＣＥ機器３に送信したサーバ乱数を特定することができる。このように、ワンタイムＩＤ１は、乱数特定情報を構成している。

ＣＥ機器３は、認証サーバ５からサーバ乱数とワンタイムＩＤ１を受信する（受信手段）。ついで、ＣＥ機器３は、共通鍵を生成してこれを認証サーバ５の公開鍵で暗号化する（ステップ４）。この情報は、ＣＥ機器３の接続先が確かに認証サーバ５であることを確認するために用いられる。

次に、ＣＥ機器３は、パスフレーズとサーバ乱数を組み合わせて所定のロジックでハッシュを取り、ダイジェストを生成する（変換手段）（ステップ６）。

次に、ＣＥ機器３は、機器ＩＤ、生成したダイジェスト、認証サーバ５から受信したワンタイムＩＤ１を認証サーバ５を送信する（送信手段）（ステップ８）。

また、これらの情報と共に、先に公開鍵で暗号化した共通鍵と、ＣＥ

機器３がサービスを受けようとしているサービスサーバ４のサイトのＵＲＬ（以下ターゲットＵＲＬと呼ぶ）、及び、共通鍵を取り出すための秘密鍵（認証サーバ５は、複数の秘密鍵を持っている）を識別する秘密鍵識別子も認証サーバ５に送信する。

認証サーバ５は、これらの情報をＣＥ機器３から受信して(受信手段)、まずワンタイムＩＤ１の確認を行う（ステップ２４）。ワンタイムＩＤ１により、認証サーバ５は、先に生成したセッションの続きであることを認識することができる。

また、ワンタイムＩＤ１にひも付けて置いたサーバ乱数を記憶装置から取得することによりサーバ乱数を特定する（乱数特定手段）。

また、機器ＩＤからＣＥ機器３のパスフレーズを特定する（秘密情報特定手段）。

更に、認証サーバ５は、ＣＥ機器３から受信したターゲットＵＲＬが、予め認証サーバ５に登録されているターゲットＵＲＬかも確認する。

これにより、ＣＥ機器３の接続先のサービスサーバ４が正当なサービスサーバ４であることを確認することができる。

次に、認証サーバ５は、先にＣＥ機器３に送信したサーバ乱数と、ＣＥ機器３のパスフレーズから、ＣＥ機器３と同じロジックによりダイジェストを生成し（変換手段）、これと、ＣＥ機器３から受信したダイジェストを照合してＣＥ機器３の認証を行う（機器認証手段）（ステップ２６）。

認証サーバ５は、認証に成功するとワンタイムＩＤ２を生成する（ステップ２８）。ワンタイムＩＤ２は、後ほどＣＥ機器３が認証を受けたのが確かに認証サーバ５であることをサービスサーバ４が確認するのに使用される。

また、認証サーバ５は、機器認証を行ったバージョンも記憶しておく。

次に、認証サーバ５は、公開鍵で暗号化された共通鍵を秘密鍵で復号化して取り出す。

そして、認証サーバ５は、ワンタイムＩＤ２をハッシュ化し、ダイジェスト（以下、ＩＤ２ダイジェストと呼ぶ）を生成する。

次に、認証サーバ５は、ＩＤ２ダイジェストを先に復号化した共通鍵で暗号する（ステップ３０）。

次に、認証サーバ５は、暗号化したＩＤ２ダイジェストと、ワンタイムＩＤ２を連結して共通鍵で暗号化し、これをＣＥ機器３に送信する（ステップ３２）。

ワンタイムＩＤ２にＩＤ２ダイジェストを連結するのは、送信されてきたワンタイムＩＤ２のダイジェストを生成して、ＩＤ２ダイジェストと比較することにより、ワンタイムＩＤ２が改変されたか否かを確認するためである。

ＣＥ機器３は、認証サーバ５から暗号化されたワンタイムＩＤ２とＩＤ２ダイジェストを受信し、共通鍵でこれらを復号化する（ステップ１０）。

ＣＥ機器３は、ワンタイムＩＤ２をハッシュ化してダイジェストを生成し、これをＩＤ２ダイジェストと比較してワンタイムＩＤ２が改竄されていないか確認する。

ＣＥ機器３は、共通鍵でこれらの情報が復号化できたことから、認証サーバ５が共通鍵を取り出せた（即ち、秘密鍵を持っている）ことを確認することができる。即ち、ＣＥ機器３が機器認証を求めた相手先は確かに認証サーバ５であった

ことを確認することができる（ステップ１２）。

また、ワンタイムＩＤ２が発行されたことから、ＣＥ機器３が機器認証されたことを確認することができる。

次に、ＣＥ機器３は、認証サーバ５から受信したワンタイムＩＤ２をサービスサーバ４に送信することにより、ＣＥ機器３が認証サーバ５で認証されたことを通知する（ステップ１４）。

サービスサーバ４は、ＣＥ機器３からワンタイムＩＤ２を受信し、これを認証サーバ５に送信して確かに認証サーバ５が機器認証したことを確認する（ステップ３４、ステップ４２）。

サービスサーバ４は、認証サーバ５で機器認証結果を確認すると、ＣＥ機器３に対してサービスの提供を開始する（ステップ４４）。

そして、ＣＥ機器３ではサービスの利用を開始する（ステップ１６）。

以上の手順により、認証サーバ５は、パスフレーズそのものではなく、パスフレーズとサーバ乱数から生成されるダイジェストによりダイジェスト認証を行うことができる。

また、ＣＥ機器３は、共通鍵を公開鍵で暗号化して認証サーバ５に送信し、認証サーバ５の秘密鍵で共通鍵が取り出されたことを確認することにより、認証先が確かに認証サーバ５であることを確認することができる。

更に、認証サーバ５は、ワンタイムＩＤ２にＩＤ２ダイジェストを貼付してＣＥ機器３に送信することにより、ＣＥ機器３は、ワンタイムＩＤ２が改竄されていないことを確認することができる。

図５は、ステップ２６（図４）のダイジェスト認証処理の手順を説明するためのフローチャートである。

認証サーバ５は、ＣＥ機器３へサーバ乱数とワンタイムＩＤ１を送信する際に、これらを対応付けて記憶している。

認証サーバ５は、ＣＥ機器３から受信したワンタイムＩＤ１を用いてＣＥ機器３に送信したサーバ乱数を検索する（ステップ５２）。

また、認証サーバ５は、機器ＩＤとパスフレーズを予め対応付けて記

憶しており、ＣＥ機器３から受信した機器ＩＤからＣＥ機器３のパスフレーズを検索する（ステップ５４）。

次に、認証サーバ５は、検索したサーバ乱数とパスフレーズの組をＣＥ機器３と同じロジックによりハッシュ化し、ダイジェストを生成する（ステップ５６）。

次に、認証サーバ５は、生成したダイジェストと、ＣＥ機器３から受信したダイジェストを比較し、同一か否かを判断する（ステップ５８）。

ダイジェストが一致した場合（ステップ６０；Ｙ）、認証サーバ５は、機器認証が成功したことを認識する（ステップ６２）。

ダイジェストが一致しなかった場合（ステップ６０；Ｎ）、認証サーバ５は、ＣＥ機器３が認証されなかったものと認識する（ステップ６４）。

以上のように、認証サーバ５は、ワンタイムＩＤとサーバ乱数を対応付けて記憶しておき、更に機器ＩＤとパスフレーズを対応付けて記憶しておくことにより、ＣＥ機器３と同じロジックでダイジェストを生成することができ、ＣＥ機器３を機器認証することができる。

図６は、ステップ３４、ステップ４２（図４）において、サービスサーバ４が認証サーバ５で認証結果を確認する手順を説明するためのフローチャートである。

以下、認証サーバ５とサービスサーバ４の通信は、ＳＳＬなどの技術により暗号化された通信経路を介して行われるものとする。

まず、サービスサーバ４は、認証サーバ５にＣＥ機器３から受信したワンタイムＩＤ２を送信し、機器認証の結果を要求する（ステップ８２）。この際に、サービスサーバ４は、認証サーバ５とのセッションを維持するためのチケットを発行し、これも認証サーバ５に送信する。

サービスサーバ４と認証サーバ５との送受信はお互いの信頼性が高いため、セッションの度にワンタイムＩＤを発行せず、同じＩＤを複数回

繰り返して使用してもよい。このように複数回再利用できるＩＤをチケットと呼ぶことにする。

ワンタイムＩＤの代わりにチケットを発行することにより、サービスサーバ４と認証サーバ５の負荷を、ワンタイムＩＤを発行した場合より小さくすることができる。

認証サーバ５は、ワンタイムＩＤ２を受信し、このワンタイムＩＤ２をキーとして、ＣＥ機器３に対して行った機器認証のバージョンを検索する。また、ＣＥ機器３の機器ＩＤなどからＣＥ機器３の機器情報も検索する。

機器情報としては、例えば、ＣＥ機器３の製品コードやシリアルナンバなどがある。

そして、これら検索した情報をサービスサーバ４に送信する（ステップ７２）。

サービスサーバ４は、バージョン情報と機器情報を認証サーバ５から受信し、サービスサーバ４で記憶しているこれらの情報と照合する。

更に、サービスサーバ４は、認証サーバ５にチケットを送信し、ＣＥ機器３の保有者情報を認証サーバ５に要求する（ステップ８４）。

認証サーバ５は、これに応じてこのＣＥ機器３の保有者情報を検索し、チケットと共にサービスサーバ４に送信する（ステップ７４）。

サービスサーバ４は、認証サーバ５から受信した保有者情報をサービスサーバ４が記憶している保有者情報と照合する。

このように、機器情報や保有者情報を確認することにより、サービスサーバ４は、認証サーバ５は、確かにＣＥ機器３を機器認証したことを確認することができる。

そして、サービスサーバ４は、ＣＥ機器３に対してサービスの提供を開始する（ステップ８６）。

以上のように、サービスサーバ４と認証サーバ５との間の複数回の送受信において同じチケットが繰り返し用いられる。

また、サービスサーバ４は、別の機器認証に関する認証結果確認には別のチケットを発行する。

図７は、ＣＥ機器３が認証先が確かに認証サーバ５であることを確認する別のシーケンスを説明するためのフローチャートである。

以下の手順では、ＣＥ機器３が乱数（以下クライアント乱数と呼ぶことにする）を発生させ、これにより認証サーバ５を確認する。

まず、ＣＥ機器３は、クライアント乱数を生成する（ステップ１０２）。

次に、ＣＥ機器３は、共通鍵を生成する（ステップ１０４）。

ＣＥ機器３は、生成した共通鍵でクライアント乱数を暗号化する（ステップ１０６）。暗号化した後の情報を暗号化情報１と呼ぶことにする。

更に、ＣＥ機器３は、認証サーバ５の公開鍵で共通鍵を暗号化する（ステップ１０８）。暗号化した後の情報を暗号化情報２と呼ぶことにする。

そして、ＣＥ機器３は、暗号化情報１と暗号化情報２を認証サーバ５に送信する（ステップ１１０）。

なお、ＣＥ機器３は、送信したクライアントを記憶しておく。

認証サーバ５は、ＣＥ機器３から暗号化情報１と暗号化情報２を受信し、まず、認証サーバ５の秘密鍵で暗号化情報２を復号化し、共通鍵を取り出す（ステップ１２２）。

次に、認証サーバ５は、取り出した共通鍵で暗号化情報１を復号化し、クライアント乱数を取り出す（ステップ１２４）。

次に、認証サーバ５は、取り出したクライアント乱数のハッシュをとり、ダイジェストを生成する（ステップ１２６）。

次に、認証サーバ５は、生成したダイジェストを共通鍵で暗号化し、ＣＥ機器３に送信する（ステップ１２８）。

ＣＥ機器３は、認証サーバ５から暗号化したダイジェストを受信し、これを共通鍵で復号化する（ステップ１１２）。

更に、ＣＥ機器３は、記憶しておいた乱数をハッシュ化し、ダイジェストを生成する（ステップ１１４）。

そして、ＣＥ機器３は、生成したダイジェストと、先に復号化したダイジェストを比較し、両者が一致することにより、接続先が確かに認証サーバ５であることを確認する（ステップ１１６）。

即ち、クライアント乱数のダイジェストが共通鍵で暗号化されて送られてきたということは、接続先が暗号化情報２を復号化することができたということであり、これは、接続先が秘密鍵を持っていたことを意味する。秘密鍵を持っているのは認証サーバ５であるので、これにより、接続先が認証サーバ５であることを確認することができる。

図８は、機器認証を行う他の手順を説明するためのフローチャートである。

図４に示した手順では、ＣＥ機器３から認証サーバ５にアクセスして機器認証を行ったが、この手順では、ＣＥ機器からサービスサーバ４に認証情報を送信し、サービスサーバ４がこの認証情報を用いて認証サーバ５にアクセスして機器認証を行う。

以下の手順で、ＣＥ機器３、サービスサーバ４、認証サーバ５の間の通信は、例えば、ＳＳＬなどの技術により暗号化した経路が用いられるものとする。

また、ＣＥ機器３、サービスサーバ４、認証サーバ５は、フローチャート中に括弧で示した各手段を備えている。

まず、ＣＥ機器３がサービスサーバ４に対して機器認証を要するサービスの提供を要求する。

これに対し、サービスサーバ４は、ＣＥ機器３に対して機器認証トリ

ガを送信する（ステップ１４２）。

ＣＥ機器３は、サービスサーバ４から機器認証トリガを受信するとサービスサーバ４に対してサーバ乱数の要求を送信する(ステップ１３２)。

サービスサーバ４は、これを受信してサーバ乱数を生成し（乱数取得手段）（ステップ１４４）、ＣＥ機器３に送信する（乱数送信手段）（ステップ１４６）。サービスサーバ４は、このサーバ乱数を記憶しておく。

ＣＥ機器３は、サービスサーバ４からサーバ乱数を受信すると共に(乱数受信手段)、クライアント乱数を生成する（ステップ１３４）。

次にＣＥ機器３は、サーバ乱数、クライアント乱数、及びパスフレーズを組み合わせてハッシュ化し、ダイジェストを生成する（変換手段）（ステップ１３６）。

次に、ＣＥ機器３は、生成したダイジェストと、機器ＩＤ、クライアント乱数をサービスサーバ４に送信して機器認証を要求する(送信手段)（ステップ１３８）。

サービスサーバ４は、これらの認証情報を受信する（受信手段）（ステップ１４８）。

このように、サービスサーバ４がＣＥ機器３から受信する認証情報には、サーバ乱数が含まれていない。

サービスサーバ４は、ＣＥ機器３から受信した認証情報（ダイジェスト、機器ＩＤ、クライアント）にサーバ乱数を加えて新たな認証情報とし、これを認証サーバ５に送信して機器認証を要求する（認証情報送信手段）（ステップ１５０）。

ここでは、サービスサーバ４は、ＣＥ機器３とセッションを維持しているため、先に記憶したサーバ乱数がこのＣＥ機器３に送ったサーバ乱数であることを認識することができる（乱数特定手段）。そこで、このサーバ乱数を認証情報に加えるのである。また、図４の手順と同様にし

てワンタイムＩＤを発行することにより、ＣＥ機器３に送信したサーバ乱数を特定するように構成することもできる。

このように、ＣＥ機器３から送られてきた認証情報に先に送信したサーバ乱数を付加するように構成することにより、認証トリガを送信したサービスサーバ４と認証情報を受信したサービスサーバ４が同一のサーバであることを確かめることができる。

認証サーバ５は、サービスサーバ４から認証情報を受信し（受信手段）、ＣＥ機器３の機器認証を行う（ステップ１６２）。

この認証では、サービスサーバ４から送信されてきた機器ＩＤ、クライアント乱数、サーバ乱数の組から、ＣＥ機器３と同じロジックでダイジェストを生成し、サービスサーバ４から送信されてきたダイジェストと一致するか否かをチェックする。

一致した場合、ＣＥ機器３は認証され、一致しない場合は認証されない。

そして、認証サーバ５は、認証結果をサービスサーバ４に送信する（ステップ１６４）。

また、ＣＥ機器３のパスフレーズは、機器ＩＤから求める（秘密情報特定手段）。

サービスサーバ４は、認証サーバ５から認証結果を受信し（認証結果受信手段）、その認証結果がＣＥ機器３を認証するものであった場合、サービスの提供を開始し（ステップ１５２）、ＣＥ機器３ではそのサービスを利用する（ステップ１４０）。

なお、ステップ１６４で認証サーバ５がサービスサーバ４に認証結果を送信する際に、図６のフローチャートと同様にして、認証サーバ５とサービスサーバ４の間でＣＥ機器３の機器情報と保有者情報を確認するように構成することもできる。

図９は、ステップ１６２（図８）のダイジェスト認証処理の手順を説明するためのフローチャートである。

まず、認証サーバ５は、サービスサーバ４から受信した認証情報に含まれる機器ＩＤを用いてＣＥ機器３のパスフレーズを検索して取得する（ステップ１７２）。なお、認証サーバ５は、予め機器ＩＤとパスフレーズを対応させて記憶している。

次に、認証サーバ５は、サービスサーバ４から受信した認証情報に含まれるサーバ乱数とクライアント乱数を取得する（ステップ１７４）。

次に、認証サーバ５は、ステップ１７２で検索したパスフレーズと、ステップ１７４で取得したサーバ乱数及びクライアント乱数を組み合わせ、ＣＥ機器３と同じロジックにてこれをハッシュ化し、ダイジェストを生成する（ステップ１７６）。

次に、認証サーバ５は、ステップ１７６で生成したダイジェストと、サービスサーバ４から受信した認証情報に含まれるダイジェストを比較し、同一であるか否かを判断する（ステップ１７８）。

ダイジェストが一致する場合（ステップ１８０；Ｙ）、認証サーバ５は、ＣＥ機器３が認証されたものと判断し（ステップ１８２）、ダイジェストが一致しない場合（ステップ１８０；Ｎ）、認証サーバ５は、ＣＥ機器３が認証されなかったものと判断する（ステップ１８４）。

図８のフローチャートで示した手順では、図４のフローチャートで示したようなワンタイムＩＤ１、ワンタイムＩＤ２を用いることなく機器認証を行うことができる。

以上に説明した本実施の形態では、以下のような効果を得ることができる。

（１）機器認証モジュール７は、サービスサーバ４が生成したサーバ乱数を用いてパスフレーズをダイジェストに変換した後これを出力するた

め、第三者が機器認証モジュール７の出力からパスフレーズを読み取ることはできない。

（２）暗号化モジュール８は、機器認証モジュール７からダイジェスト化されたパスフレーズを受信するため、機器認証モジュール７と暗号化モジュール８をスタティックリンクにより結合する必要がない。そのため、機器認証モジュール７と暗号化モジュール８をダイナミックリンクで接続するように構成し、暗号化モジュール８を他のモジュールからも利用できるようにすることができる。

（３）暗号化モジュール８は、機器認証モジュール７も含め他のモジュールと共用できるため、暗号化モジュール８を複数用意する必要が無く、ＣＥ機器３のシステムの冗長性を解消することができる。そのため、ＣＥ機器３のメモリ領域を有効利用することができる。

（４）認証サーバ５とＣＥ機器３で同じロジックにてダイジェストを生成することにより、ＣＥ機器３が生成したダイジェストと認証サーバ５が生成したダイジェストの一致を判断することにより機器認証を行うことができる。

（５）パスフレーズそのものではなく、機器認証ごとに値が変化するダイジェストが通信経路で送受信されるため、例えダイジェストがネットワーク上で第三者に奪取されたとしても、被害を小さい範囲にとどめることができる。即ち、パスフレーズは、機器認証で同じものが何回でも使用できるのに対し、ダイジェストは機器認証ごとに異なるからである。

（実施の形態の変形例）

図１０は、本実施の形態の変形例を説明するための図である。

図に示したように、本変形例では、機器認証モジュール７を耐タンパチップ３５に格納する。

耐タンパチップ３５は、集積回路を収納したＩＣチップによって構成

された耐タンパ装置であって、改竄や複製、内部の論理構造の解読などの不正行為に対して十分な防御手段を講じてある。

タンパ（ｔａｍｐｅｒ）とは、装置を勝手にいじったり手を加えたりするという意味であり、情報などを不正に変更するという意味もある。

耐タンパチップ３５は、機器ＩＤとパスフレーズ、及び、パスフレーズとサーバ乱数を組み合わせた情報をハッシュ化するハッシュ化機が内蔵された一種のブラックボックスとなっている。

耐タンパチップ３５は、耐タンパ仕様で製造されているため、第三者は、耐タンパチップ３５を物理的に分解して内部の情報を得ることは困難である。

即ち、耐タンパチップ３５を物理的に分解して、秘密情報であるパスフレーズや、ハッシュ化に用いるハッシュ関数を知ることは困難である。

また、耐タンパチップ３５内のパスフレーズは、サーバ乱数と共にハッシュ化されたダイジェストとして出力されるため、耐タンパチップ３５から出力された情報からパスフレーズを解析することも困難である。即ち、ハッシュ関数は一方向性関数であり、逆変換が困難だからである。

このように、耐タンパチップ３５の出力情報から内部の秘密情報を探知することも困難である。

図１１は、本変形例のハードウェア的な構成の一例を示した図である。

図に示したように、耐タンパチップ３５は、バス２４に接続しており、ＣＰＵ２１から情報の入出力を行えるようになっている。

即ち、ＣＰＵ２１は、耐タンパチップ３５に対して、サーバ乱数を入力し、耐タンパチップ３５から機器ＩＤとダイジェストを受け取ることができる。

以上のように、耐タンパチップ３５に、パスフレーズ（秘密情報）とハッシュ化機を内蔵し、パスフレーズを出力する際には、ハッシュ化し

たダイジェストを出力することにより、第三者の手にパスフレーズが渡ることを防ぐことができる。

このように、耐タンパ装置に、秘密情報とこの秘密情報の変換機能を内蔵し、耐タンパ装置から秘密情報が出力される場合は、変換機能で変換された値が出力されるように構成することにより、秘密情報を物理的、及び解析的に探索することが困難になる。そのため、セキュリティレベルを強化することができる。

本変形例では、一例として、耐タンパチップ３５にパスフレーズとハッシュ化機を内蔵した例について説明したが、この他に、例えば、秘密鍵や共通鍵などの暗号鍵情報を用いるシステムでは、これらの暗号鍵情報と、入力情報に対する署名機能や暗号化機能を耐タンパ装置に内蔵することにより、暗号鍵情報の漏洩を防ぐことができる。

産業上の利用可能性

本発明によれば、端末機器内のメモリを有効利用することができる。

請求の範囲

1． 機器認証用の秘密情報を備えた端末機器と、前記秘密情報とを用いて前記端末機器の機器認証を行う認証サーバから構成された機器認証システムであって、

前記端末機器は、乱数を取得し、前記取得した乱数と前記秘密情報との組を一方向性関数により変換して変換値を生成し、

前記認証サーバは、前記端末機器が取得した乱数、前記端末機器の秘密情報、及び前記端末機器が生成した変換値を取得し、

前記取得した乱数と秘密情報との組を前記端末機器が用いた一方向性関数と同じ一方向性関数により変換して変換値を生成し、

前記端末機器装置において生成した変換値と、前記認証サーバにおいて生成した変換値を比較することにより前記端末機器の機器認証を行うことを特徴とする機器認証システム。

2． 請求項1の機器認証システムで機器認証を受ける端末機器であって、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、

前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、

前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、

を具備したことを特徴とする端末機器。

3． 請求項2に記載の端末機器を機器認証する認証サーバであって、

乱数を取得する乱数取得手段と、

前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に

送信する送信手段と、

前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受信する受信手段と、

前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定手段と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、

前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換手段と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、

を具備したことを特徴とする認証サーバ。

4． 請求項1の機器認証システムは、認証サーバによる認証を経て前記端末機器にサービスを提供するサービスサーバを含み、

前記サービスサーバは、

乱数を取得する乱数取得手段と、

前記取得した乱数を端末機器に送信する乱数送信手段と、

前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信手段と、

前記端末機器に送信した乱数を特定する乱数特定手段と、

前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信手段と、

前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信手段と、

を具備したことを特徴とするサービスサーバ。

5． 請求項4に記載のサービスサーバからサービスの提供を受ける端

末機器であって、

サービスサーバから乱数を受信する乱数受信手段と、

前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、

前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、

を具備したことを特徴とする端末機器。

6．　請求項4に記載のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバであって、

サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信手段と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、

前記受信した乱数前記と特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換手段と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、

を具備したことを特徴とする認証サーバ。

7．　請求項1の機器認証システムで機器認証を受ける端末機器で用いる端末機器方法であって、前記端末機器は、受信手段と、変換手段と、送信手段と、備えたコンピュータから構成されており、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を前記受信手段で受信する受信ステップと、

前記受信した乱数と秘密情報の組を一方向性関数により前記変換手段で変換して変換値を生成する変換ステップと、

前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、

から構成されたことを特徴とする端末機器方法。

8．　請求項２に記載の端末機器を機器認証する認証サーバで用いる認証方法であって、前記認証サーバは、乱数取得手段と、送信手段と、受信手段と、乱数特定手段と、秘密情報特定手段と、変換手段と、機器認証手段と、

を備えたコンピュータから構成されており、

前記乱数取得手段で乱数を取得する乱数取得ステップと、

前記取得した乱数と、当該乱数を特定する乱数特定情報を前記送信手段で端末機器に送信する送信ステップと、

前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を前記受信手段で受信する受信ステップと、

前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を前記秘密情報特定手段で特定する秘密情報特定ステップと、

前記特定した秘密情報と乱数の組を、前記変換手段で前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、

前記受信した変換値と前記生成した変換値を用いて前記機器認証手段で前記端末機器を機器認証する機器認証ステップと、

から構成されたことを特徴とする認証方法。

9．　請求項４に記載のサービスサーバで用いる認証方法であって、前記サービスサーバは、乱数取得手段と、乱数送信手段と、受信手

段と、乱数特定手段と、認証情報送信手段と、認証結果受信手段と、を備えたコンピュータから構成されており、

前記乱数取得手段で乱数を取得する乱数取得ステップと、

前記取得した乱数を前記乱数送信手段で端末機器に送信する乱数送信ステップと、

前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を前記受信手段で受信する受信ステップと、

前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、

前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を前記認証情報送信手段で認証サーバに送信する認証情報送信ステップと、

前記認証サーバから前記送信した認証情報による認証結果を前記認証結果受信手段で受信する認証結果受信ステップと、

から構成されたことを特徴とする認証方法。

１０．　請求項４に記載のサービスサーバからサービスの提供を受ける端末機器で用いる端末機器方法であって、前記端末機器は、乱数受信手段と、変換手段と、送信手段とを備えたコンピュータから構成されており、

前記乱数受信手段でサービスサーバから乱数を受信する乱数受信ステップと、

前記受信した乱数と、秘密情報の組を前記変換手段で一方向性関数により変換して変換値を生成する変換ステップと、

前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、

から構成されたことを特徴とする端末機器方法。

１１．　請求項４に記載のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバが用いる認証方法であって、前記認証サーバは、受信手段と、秘密情報特定手段と、変換手段と、機器認証手段と、を備えたコンピュータから構成されており、

サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を前記受信手段で受信する受信ステップと、

前記秘密情報特定手段で、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定ステップと、

前記受信した乱数前記と特定した秘密情報との組を前記変換手段で前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、

前記機器認証手段で、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証ステップと、

から構成されたことを特徴とする認証方法。

１２．　請求項１の機器認証システムで機器認証を受けるコンピュータで構成された端末機器において、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信機能と、

前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換機能と、

前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、

を実現する端末機器プログラム。

１３．　請求項２に記載の端末機器を機器認証するコンピュータで構成された認証サーバにおいて、

乱数を取得する乱数取得機能と、

前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に送信する送信機能と、

前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受信する受信機能と、

前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定機能と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、

前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換機能と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、

を実現する認証プログラム。

１４．　請求項４に記載のコンピュータで構成されたサービスサーバにおいて、

乱数を取得する乱数取得機能と、

前記取得した乱数を端末機器に送信する乱数送信機能と、

前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信機能と、

前記端末機器に送信した乱数を特定する乱数特定機能と、

前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信機能と、

前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信機能と、

を実現するサービスサーバプログラム。

１５．　請求項４に記載のサービスサーバからサービスの提供を受けるコンピュータで構成された端末機器において、

サービスサーバから乱数を受信する乱数受信機能と、

前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換機能と、

前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、

を実現する端末機器プログラム。

１６．　請求項４に記載のサービスサーバがサービスを提供する際に、端末機器を機器認証するコンピュータで構成された認証サーバにおいて、

サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信機能と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、

前記受信した乱数前記と特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換機能と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、

を実現する認証プログラム。

１７．　請求項１２、又は請求項１５に記載の端末機器プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

１８．　請求項１３、又は請求項１６に記載の認証プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

１９．　請求項１４に記載のサービスサーバプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

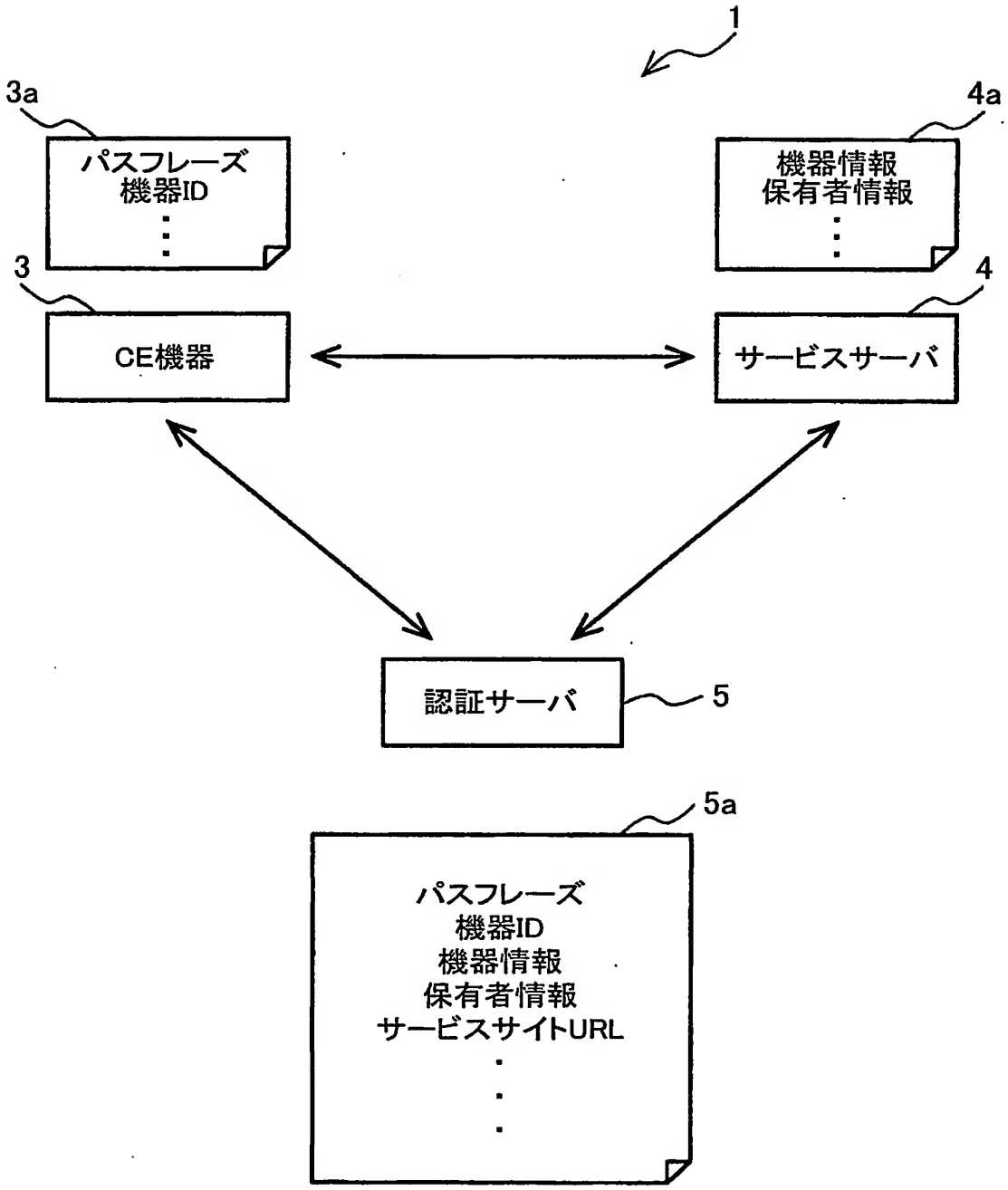

1
3a
パスフレーズ
機器ID
3
CE機器
4a
機器情報
保有者情報
4
サービスサーバ
認証サーバ
5
5a
パスフレーズ
機器ID
機器情報
保有者情報
サービスサイトURL

Fig.1

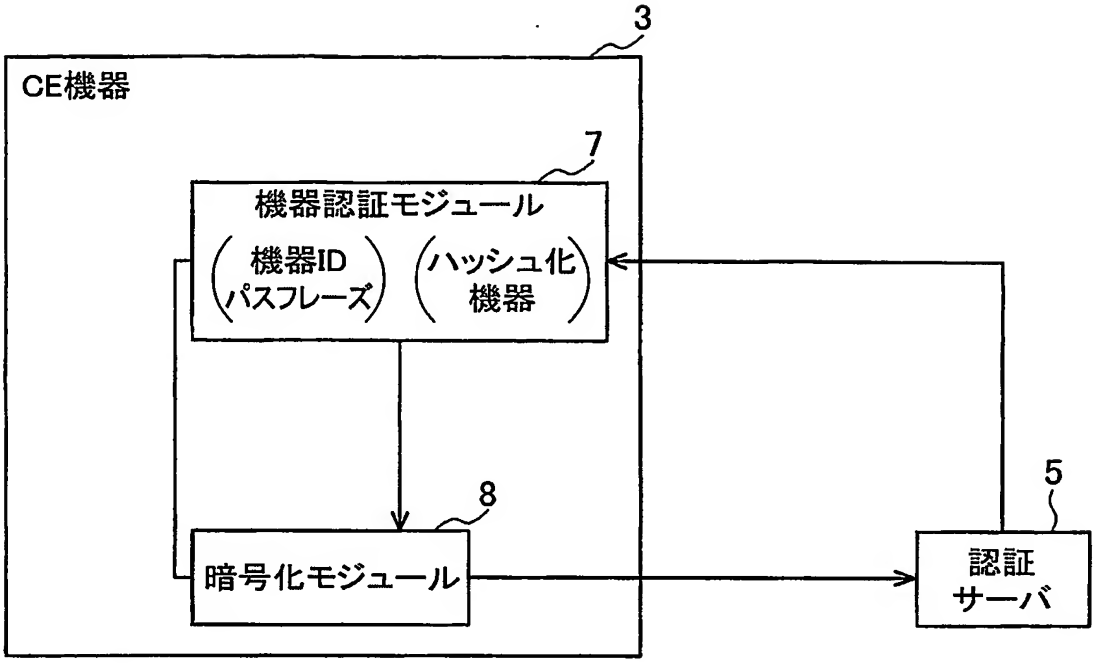

3
CE機器
7
機器認証モジュール
機器ID
パスフレーズ
ハッシュ化
機器
8
暗号化モジュール
5
認証
サーバ

Fig.2

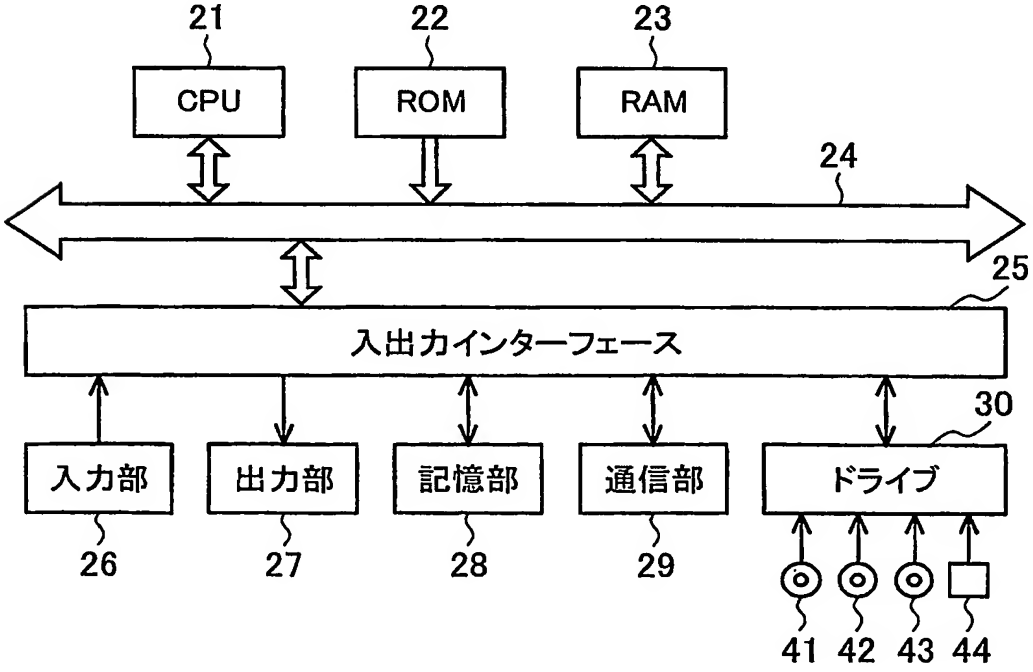

21
22
23
CPU
ROM
RAM
24
25
入出力インターフェース
30
入力部
出力部
記憶部
通信部
ドライブ
26
27
28
29
41
42
43
44

Fig.3

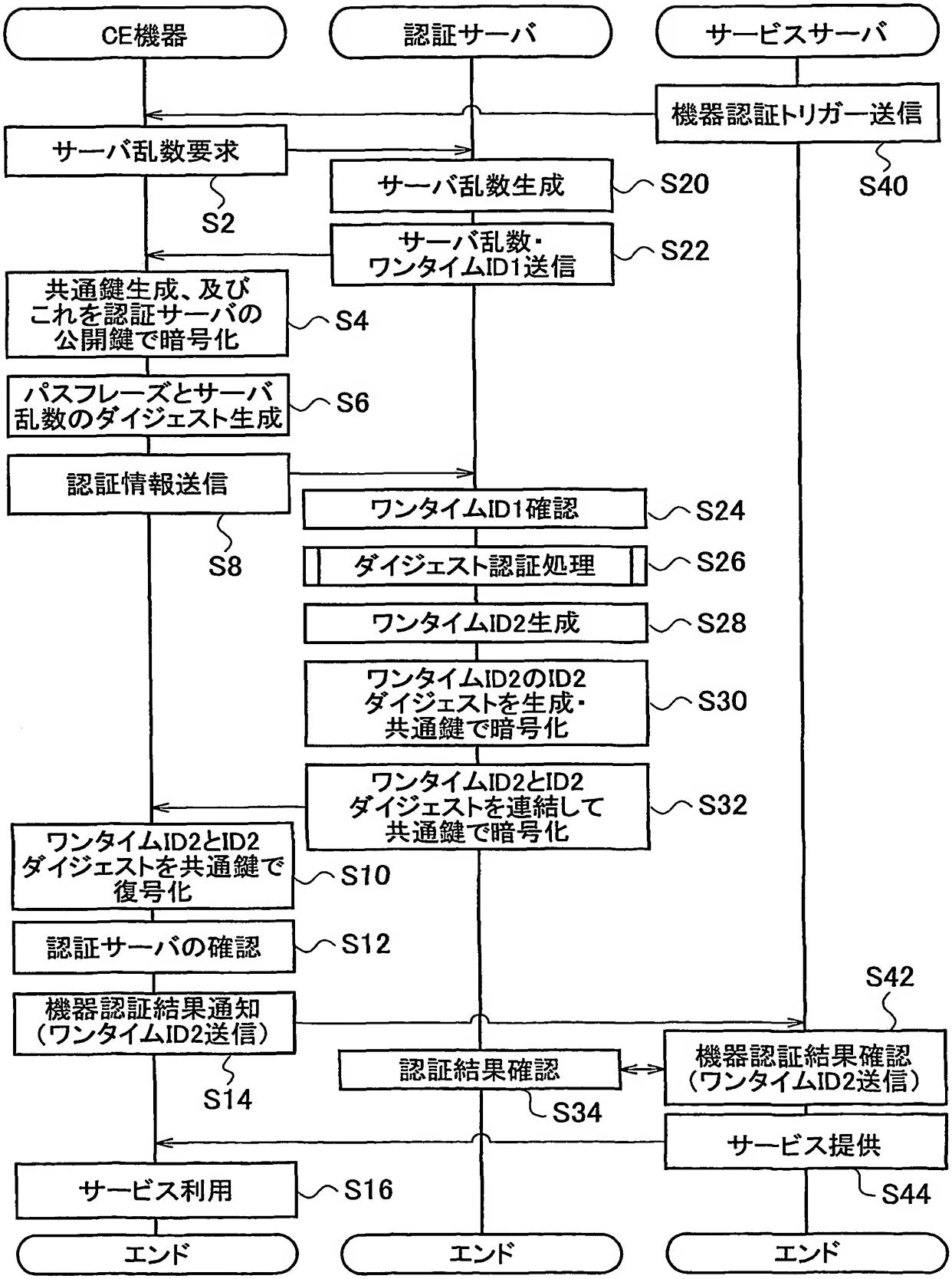

CE機器
認証サーバ
サービスサーバ
機器認証トリガー送信
S40
サーバ乱数要求
S2
サーバ乱数生成
S20
サーバ乱数・
ワンタイムID1送信
S22
共通鍵生成、及び
これを認証サーバの
公開鍵で暗号化
S4
パスフレーズとサーバ
乱数のダイジェスト生成
S6
認証情報送信
S8
ワンタイムID1確認
S24
ダイジェスト認証処理
S26
ワンタイムID2生成
S28
ワンタイムID2のID2
ダイジェストを生成・
共通鍵で暗号化
S30
ワンタイムID2とID2
ダイジェストを連結して
共通鍵で暗号化
S32
ワンタイムID2とID2
ダイジェストを共通鍵で
復号化
S10
認証サーバの確認
S12
S42
機器認証結果通知
(ワンタイムID2送信)
S14
認証結果確認
S34
機器認証結果確認
(ワンタイムID2送信)
サービス提供
S44
サービス利用
S16
エンド
エンド
エンド

Fig.4

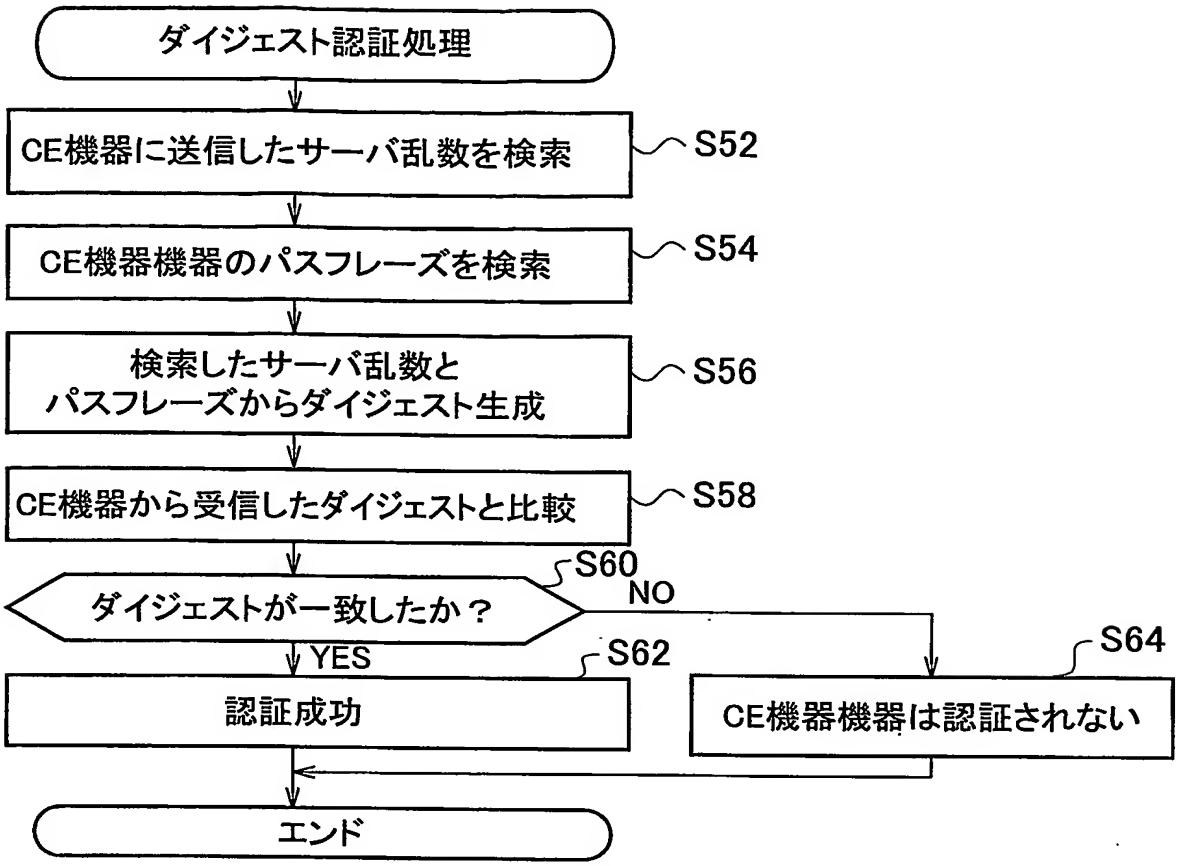

ダイジェスト認証処理
CE機器に送信したサーバ乱数を検索
S52
CE機器機器のパスフレーズを検索
S54
検索したサーバ乱数と
パスフレーズからダイジェスト生成
S56
CE機器から受信したダイジェストと比較
S58
S60
ダイジェストが一致したか？
NO
YES
S62
認証成功
S64
CE機器機器は認証されない
エンド

Fig.5

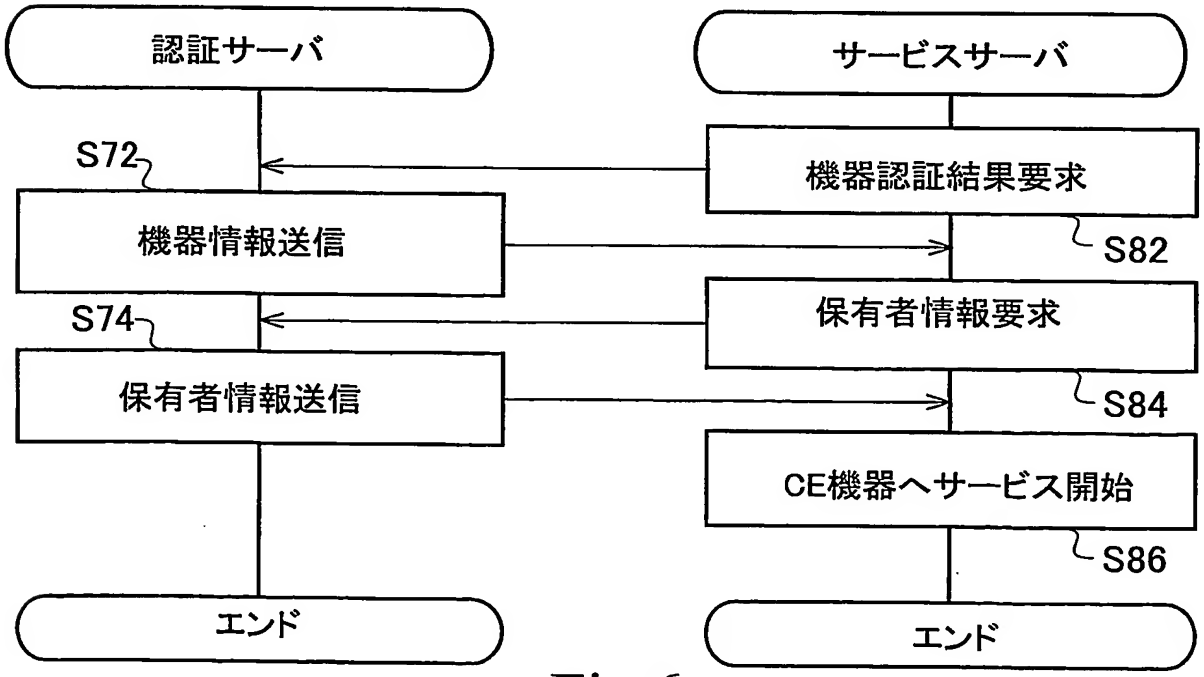

認証サーバ
サービスサーバ
S72
機器認証結果要求
機器情報送信
S82
保有者情報要求
S74
保有者情報送信
S84
CE機器へサービス開始
S86
エンド
エンド

Fig.6

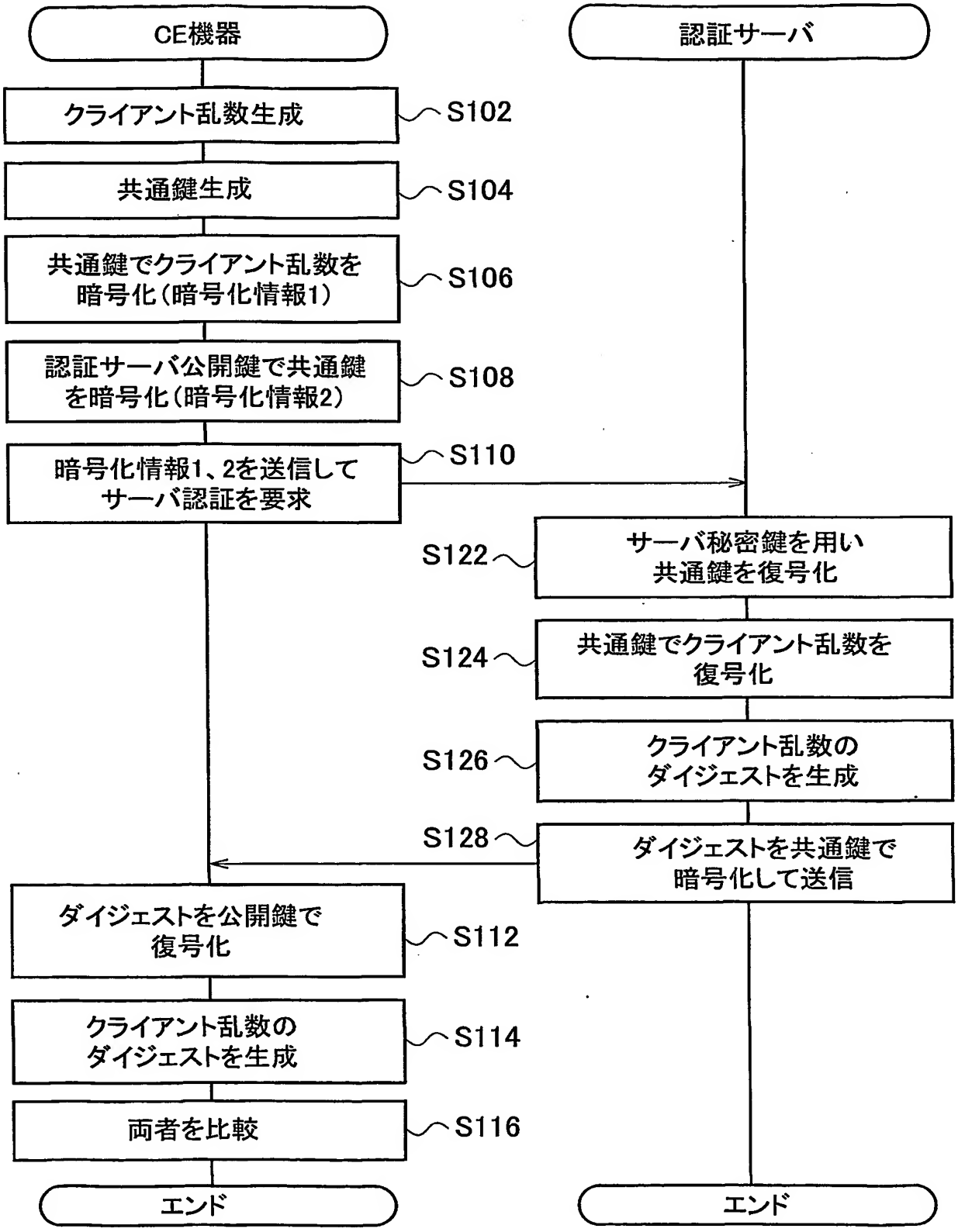

CE機器
認証サーバ
クライアント乱数生成
S102
共通鍵生成
S104
共通鍵でクライアント乱数を暗号化(暗号化情報1)
S106
認証サーバ公開鍵で共通鍵を暗号化(暗号化情報2)
S108
暗号化情報1、2を送信してサーバ認証を要求
S110
S122
サーバ秘密鍵を用い共通鍵を復号化
S124
共通鍵でクライアント乱数を復号化
S126
クライアント乱数のダイジェストを生成
S128
ダイジェストを共通鍵で暗号化して送信
ダイジェストを公開鍵で復号化
S112
クライアント乱数のダイジェストを生成
S114
両者を比較
S116
エンド
エンド

Fig.7

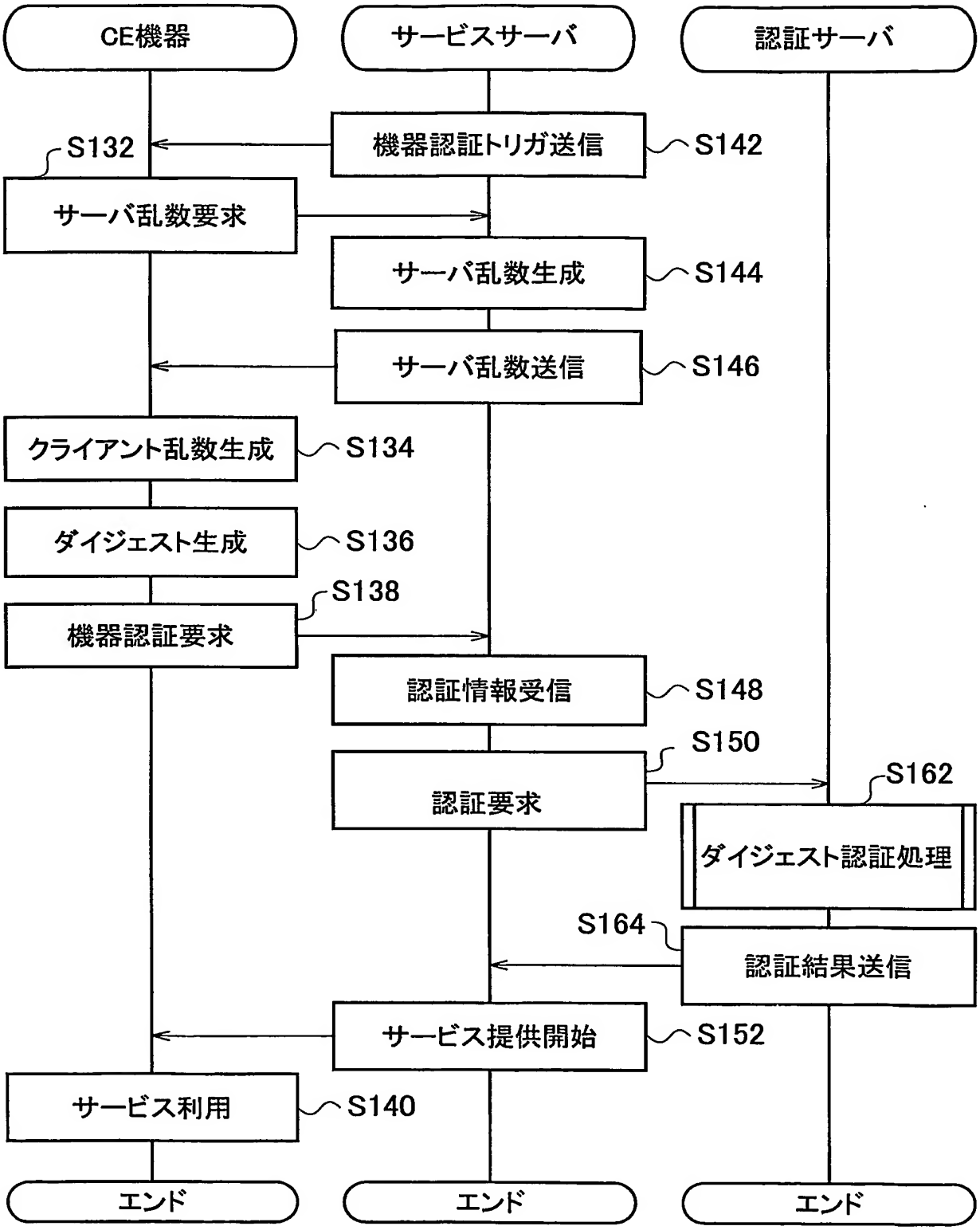

CE機器
サービスサーバ
認証サーバ
S132
機器認証トリガ送信
S142
サーバ乱数要求
サーバ乱数生成
S144
サーバ乱数送信
S146
クライアント乱数生成
S134
ダイジェスト生成
S136
S138
機器認証要求
認証情報受信
S148
S150
認証要求
S162
ダイジェスト認証処理
S164
認証結果送信
サービス提供開始
S152
サービス利用
S140
エンド
エンド
エンド

Fig.8

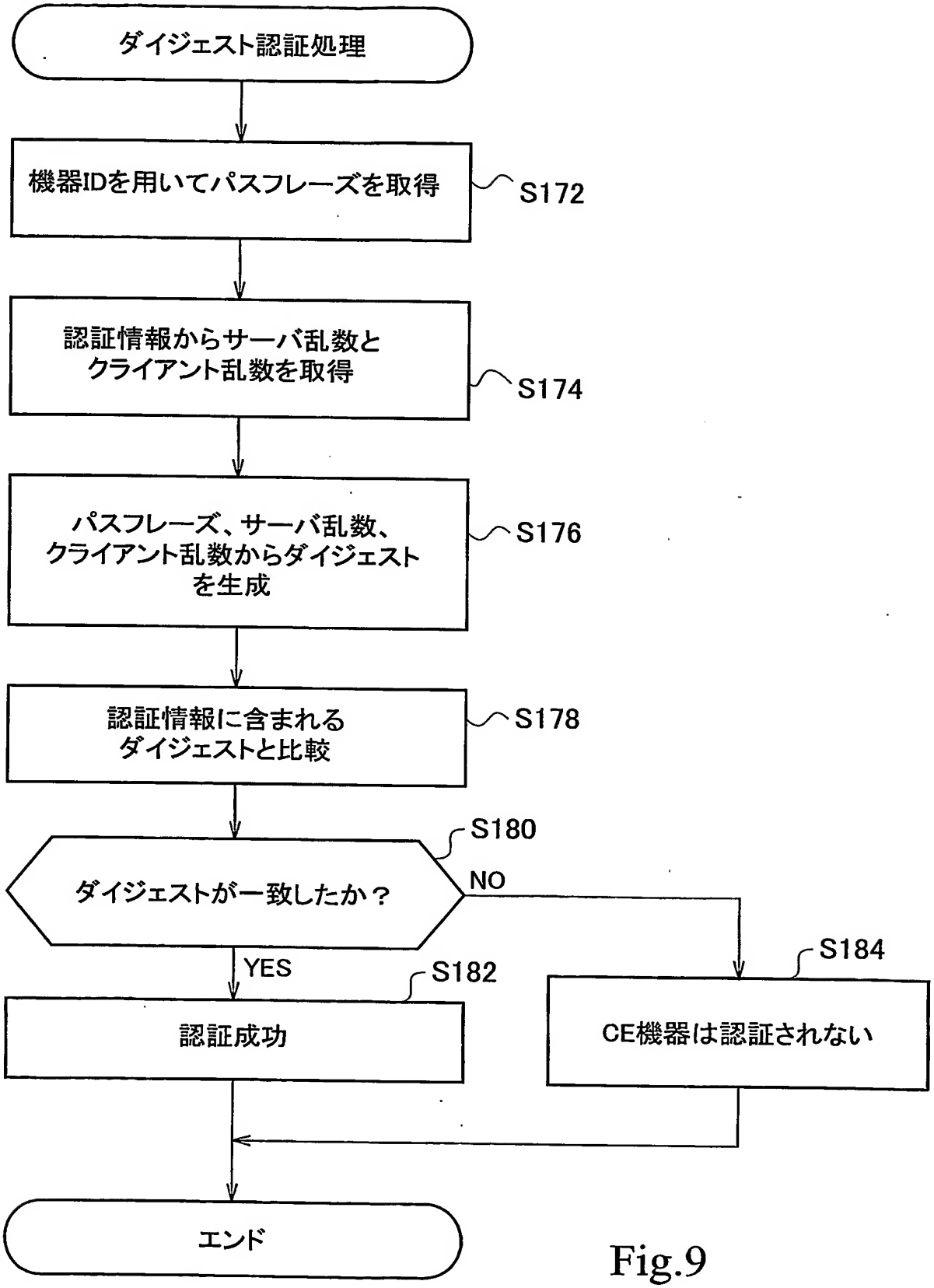

ダイジェスト認証処理
機器IDを用いてパスフレーズを取得
S172
認証情報からサーバ乱数と
クライアント乱数を取得
S174
パスフレーズ、サーバ乱数、
クライアント乱数からダイジェスト
を生成
S176
認証情報に含まれる
ダイジェストと比較
S178
S180
ダイジェストが一致したか？
NO
YES
S182
認証成功
S184
CE機器は認証されない
エンド

Fig.9

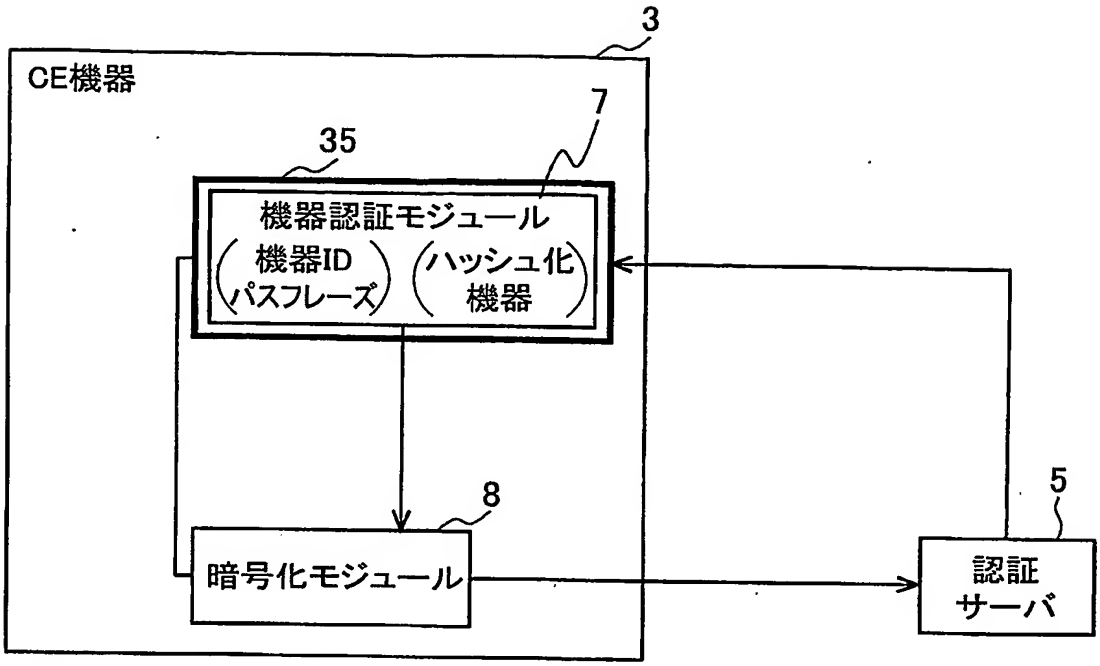

3
CE機器
7
35
機器認証モジュール
機器ID
パスフレーズ
ハッシュ化
機器
8
暗号化モジュール
5
認証
サーバ

Fig.10

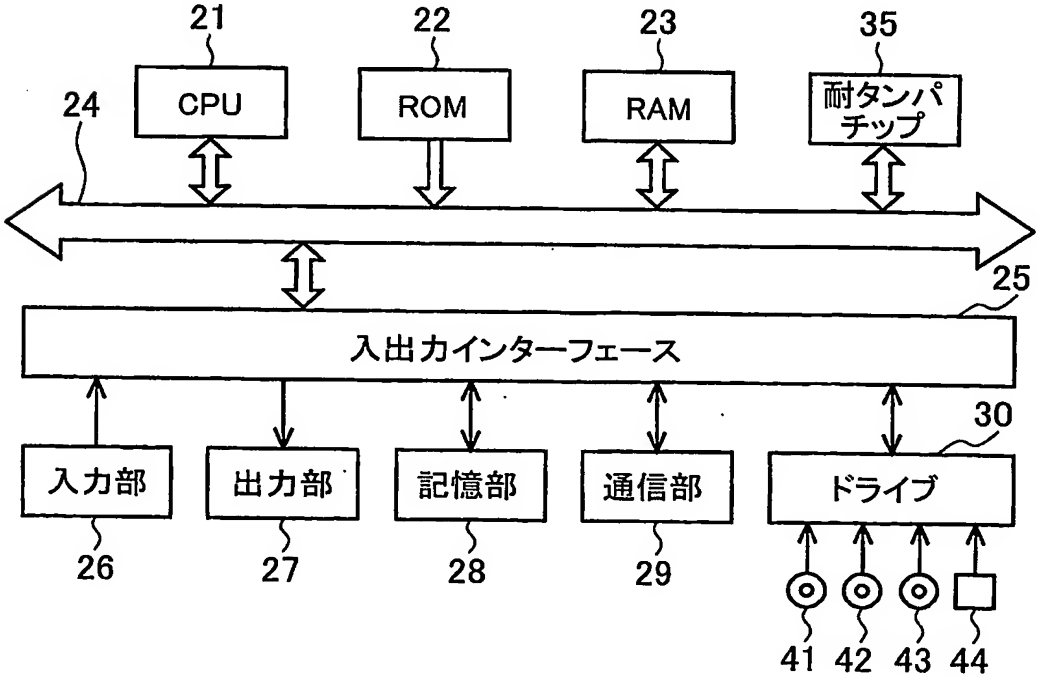

21
CPU
22
ROM
23
RAM
35
耐タンパ
チップ
24
25
入出力インターフェース
30
入力部
出力部
記憶部
通信部
ドライブ
26
27
28
29
41
42
43
44

Fig.11

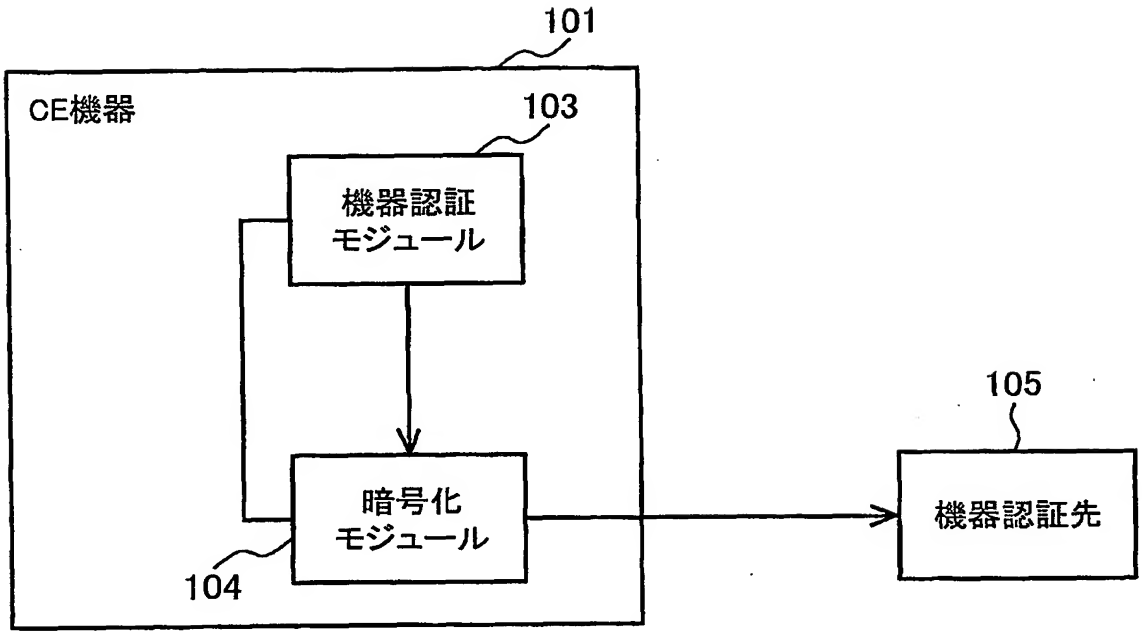


Fig.12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/005741

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/32, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 11-316729 A (Nippon Telegraph And Telephone Corp.), 16 November, 1999 (16.11.99), Par. Nos. [0032] to [0038]; Fig. 5 & EP 921487 A & US 6343284 B	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 May, 2004 (21.05.04)	08 June, 2004 (08.06.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/005741

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 2-19
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

(See extra sheet.)

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.II-2 of continuation of first sheet(2)

The scope of claim 2 contains a description of "a terminal device receiving a device authentication by the device authentication system of claim 1 characterized in that ..... Herein, even if "claim 1" means "the scope of claim 1", "the scope of dependent claim" is "the scope of claim" containing all the features of one or more other scopes of claims (PCT Rule 6.4 (a)). However, "a terminal device" cannot have all the features of the "device authentication system". Accordingly, the scope of claim 2 cannot be the scope of claim dependent on claim 1. Moreover, it is unclear what kind of meaning is contained in the technical feature that the terminal device receives a device authentication from a device authentication system characterized by performing authentication by a particular procedure when specifying the "terminal device". Accordingly, such a description makes unclear the feature for specifying the invention.

The same applies to the scopes of claims 3-19.

国際調査報[redacted]　　国際出願番号　P[redacted]／JP2004／005741

A.　発明の属する分野の分類（国際特許分類（IPC））

Int.Cl⁷ H04L9/32, G06F15/00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl⁷ H04L9/32, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 11-316729 A（日本電信電話株式会社）1999.11.16, 段落【0032】－【0038】，図5 & EP 921487 A & US 6343284 B	1

☐ C欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　21.05.2004	国際調査報告の発送日　08.6.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5M　3365 中里　裕正 電話番号　03－3581－1101　内線　3597

第１ページの続葉（２）第Ⅱ欄　２．のつづき

請求の範囲第２項には、「請求項１の機器認証システムで機器認証を受ける端末装置であって、...端末装置」と記載されている。ここで、「請求項１」なるものが、「請求の範囲第１項」の意味であるにしても、「従属請求の範囲」とは、１又は２以上の他の請求の範囲の全ての特徴を含む請求の範囲である（ＰＣＴ規則６．４（ａ））ところ、「端末装置」が「機器認証システム」の全ての特徴を含むはずも無いから、かかる請求の範囲第２項は、請求の範囲第１項の従属請求の範囲ではない。そして、端末装置が、特定の手続きにて認証を行うことを特徴とする機器認証システムで機器認証を受けるものであるということが、「端末装置」を特定する上でどのような意味を有するのか不明であるから、かかる記載は発明を特定するための事項を著しく不明確にするものである。

請求の範囲第３－１９項についても同様である。

国際調査報[redacted]　　国際出願番号　P[redacted]／ＪＰ２００４／００５７４１

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☒ 請求の範囲 ＿＿２－１９＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
別紙参照。

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意
☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。